EXHIBIT C-4
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 6 ('661 Patent)	**U.S. 4,932,053 to Fruhauf et al. ("Fruhauf")**
A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	Abstract – "The disclosure concerns the safety of the confidential information contained in integrated circuits. In a certain number of integrated circuit applications and, more particularly, in the circuits contained in cards known as 'chip cards', it is necessary to prohibit access by unauthorized persons to confidential information stored in a memory of the circuit. To prevent the fraudulent practice of examining the current consumption at the terminals of the integrated circuit during an operation of reading or writing in the memory, a protection circuit is used." 1:11-15 – "In a certain number of integrated circuit applications and, more particularly, in the circuits contained in cards known as 'chip cards', it is necessary to prohibit access by unauthorized persons to confidential information stored in a memory of the circuit." 1:59-2:3 – "Consequently, it is possible to partially or totally decipher the confidential content of a memory by observing the current consumed during the reading or writing of this memory. A user with fraudulent intent could measure the current consumed between the general supply terminals (necessarily accessible outside the integrated circuit). As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit." 2:4-12 – "Another example of fraud, this time concerning the writing and not the reading of confidential information, would be the following one: in certain protected circuits, there is provision for the user to introduce an enabling code through a keyboard whenever he wishes to use the circuit. To prevent fraud involving all the systematic introduction of every possible code, there is provision for storing an error bit in the memory whenever a wrong code is introduced." 2:29-40 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells

	having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:59-62 – "Consequently, it is possible to partially or totally decipher the confidential content of a memory by observing the current consumed during the reading or writing of this memory." 1:66-2:3 – "As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit." 2:6-9 – "Another example of fraud, this time concerning the writing and not the reading of confidential information, would be the following one: in certain protected circuits, there is provision for the user to introduce an enabling code through a keyboard whenever he wishes to use the circuit." 2:23-26 – "The present invention seeks to prevent these possibilities of fraudulent behaviour, chiefly in the reading but also, as the case may be, in the writing of confidential information."
(b) a source of unpredictable information;	2:29-40 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of

	the integrated circuit." 2:67-3:5 – "The pseudo-random generator could be made in a standard way by a series of cascade-mounted flip-flops, the outputs of certain flip-flops being looped back to the inputs of other flip-flops through OR-Exclusive gates. The random character may again be reinforced by the random variation of the clock frequency which controls these flip-flops." 3:14-16 – "FIG. 2 shows an example of a pseudo-random sequences generator which can be used in the protection circuit according to the invention . . . ." 3:17-20 – "FIG. 3 is a block diagram indicating how the generator of pseudo-random sequences may be controlled by an oscillator, the frequency of which is itself controlled by outputs of the generator . . . ." 3:31-35 – "It essentially comprises several simulation cells (three cells herein) controlled, through respective D-type flip-flops, BD1 for the first cell, BD2 for the second cell and BD3 for the third cell, by three outputs S1, S2, S3 of a pseudo-random sequences generator GPA." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit." Figures 2, 3.
(c) a processor:	1:23-27 – "In practice, it has therefore been provided that, when the degree of confidentiality is especially high, the confidential information is processed by a microprocessor contained in the same integrated circuit as the memory." 2:29-31 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form. . . ." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current

	consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."
(i) connected to said input interface for receiving and cryptographically processing said quantity,	2:4-9 – "Another example of fraud, this time concerning the writing and not the reading of confidential information, would be the following one: in certain protected circuits, there is provision for the user to introduce an enabling code through a keyboard whenever he wishes to use the circuit." 1:66-2:3 – "As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit."
(ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional electricity in said microchip during said processing; and	2:29-45 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit. The consumption read from the external terminals of the circuit will, in effect, be the superimposition of the real consumption of the memory cells and the pseudo-random consumption of the cells of the protection circuit." 3:36-38 – "Each simulation cell is designed to consume either a first current or a second current depending on the output logic level of the flip-flop that controls it." 3:58-65 – "The simulation transistors are preferably given dimensions such that their consumption (current I) is substantially identically to the consumption of a memory cell of the circuit to be protected (not shown) at the time when this cell is read (if it is sought to protect the confidentiality of information during reading) or written (if it is sought to protect the confidentiality of information during writing)." 4:12-15 – "The current consumption of the cells is controlled by the outputs S1, S2, S3 of the generator of pseudo-random sequences which gives bits, at these outputs, that are randomly (in fact, pseudo-

	randomly) 0 or 1 bits." 4:22-26 – "In this way, the pseudo-random bits generated at the outputs S1, S2, S3, are transmitted to the transistors only at the rising edge of this clock signal HL, i.e. at the instant when the current for reading or writing the memory cells to be protected will be consumed." 5:26-38 – "Depending on the state of the bits S1, S2, S3, Sa, Sb, the frequency F will assume one of 32 possible values. The sequences of pseudo-random bits, present notably at the outputs S1, S2, S3, will be therefore produced at a frequency that itself varies randomly. This reinforces the random character of the bits produced at the outputs S1, S2, S3, hence the random character of the current consumption of the protection circuit according to the invention. We thus arrive at a very efficient level of protection against the detection of confidential information by the reading of the current consumed at the terminals of an integrated circuit during an operation for reading or writing this information."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	3:12-14 – "The present invention seeks to prevent the possibilities of fraudulent use, principally during reading but also optionally of fraudulent use relating to the writing of confidential information."

Claim 9 ('661 Patent)	**U.S. 4,932,053 to Fruhauf**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	Abstract – "The disclosure concerns the safety of the confidential information contained in integrated circuits. In a certain number of integrated circuit applications and, more particularly, in the circuits contained in cards known as 'chip cards', it is necessary to prohibit access by unauthorized persons to confidential information stored in a memory of the circuit. To prevent the fraudulent practice of examining the current consumption at the terminals of the integrated circuit during an operation of reading or writing in the memory, a protection circuit is used." 1:11-15 – "In a certain number of integrated circuit applications and, more particularly, in the circuits contained in cards known as "chip cards", it is necessary to prohibit access by unauthorized persons to confidential information stored in a memory of the circuit."

	1:59-2:3 – "Consequently, it is possible to partially or totally decipher the confidential content of a memory by observing the current consumed during the reading or writing of this memory. A user with fraudulent intent could measure the current consumed between the general supply terminals (necessarily accessible outside the integrated circuit). As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit." 2:4-12 – "Another example of fraud, this time concerning the writing and not the reading of confidential information, would be the following one: in certain protected circuits, there is provision for the user to introduce an enabling code through a keyboard whenever he wishes to use the circuit. To prevent fraud involving all the systematic introduction of every possible code, there is provision for storing an error bit in the memory whenever a wrong code is introduced." 2:29-40 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being	1:59-62 – "Consequently, it is possible to partially or totally decipher the confidential content of a memory by observing the current consumed during the reading or writing of this memory." 1:66-2:3 – "As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential

representative of at least a portion of a message;	programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit." 2:6-9 – "Another example of fraud, this time concerning the writing and not the reading of confidential information, would be the following one: in certain protected circuits, there is provision for the user to introduce an enabling code through a keyboard whenever he wishes to use the circuit." 2:23-26 – "The present invention seeks to prevent these possibilities of fraudulent behaviour, chiefly in the reading but also, as the case may be, in the writing of confidential information."
(b) a source of unpredictable information;	2:29-40 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit." 2:67-3:5 – "The pseudo-random generator could be made in a standard way by a series of cascade-mounted flip-flops, the outputs of certain flip-flops being looped back to the inputs of other flip-flops through OR-Exclusive gates. The random character may again be reinforced by the random variation of the clock frequency which controls these flip-flops." 3:14-16 – "FIG. 2 shows an example of a pseudo-random sequences generator which can be used in the protection circuit according to the invention . . . ." 3:17-20 – "FIG. 3 is a block diagram indicating how the generator of pseudo-random sequences may be controlled by an oscillator, the frequency of which is itself controlled by outputs of the generator . . . ." 3:31-35 – "It essentially comprises several simulation cells (three cells herein) controlled, through respective D-type flip-flops, BD1 for the first cell, BD2 for the second cell and BD3 for the third cell, by three outputs S1, S2, S3 of a pseudo-random sequences generator GPA." Claim 1 – "A circuit for the protection of confidential data of a

	memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit." Figures 2, 3.
(c) a processor:	1:23-27 – "In practice, it has therefore been provided that, when the degree of confidentiality is especially high, the confidential information is processed by a microprocessor contained in the same integrated circuit as the memory." 2:29-31 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form. . . ." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."
(i) connected to said input interface for receiving and cryptographically processing said quantity,	2:4-9 – "Another example of fraud, this time concerning the writing and not the reading of confidential information, would be the following one: in certain protected circuits, there is provision for the user to introduce an enabling code through a keyboard whenever he wishes to use the circuit." 1:66-2:3 – "As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit."
(ii) configured to use said unpredictable information to	2:29-45 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells

conceal a correlation between externally monitorable signals and said secret during said processing of said quantity;	having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit. The consumption read from the external terminals of the circuit will, in effect, be the superimposition of the real consumption of the memory cells and the pseudo-random consumption of the cells of the protection circuit." 3:36-38 – "Each simulation cell is designed to consume either a first current or a second current depending on the output logic level of the flip-flop that controls it." 3:58-65 – "The simulation transistors are preferably given dimensions such that their consumption (current I) is substantially identically to the consumption of a memory cell of the circuit to be protected (not shown) at the time when this cell is read (if it is sought to protect the confidentiality of information during reading) or written (if it is sought to protect the confidentiality of information during writing)." 4:12-15 – "The current consumption of the cells is controlled by the outputs S1, S2, S3 of the generator of pseudo-random sequences which gives bits, at these outputs, that are randomly (in fact, pseudo-randomly) 0 or 1 bits." 4:22-26 – "In this way, the pseudo-random bits generated at the outputs S1, S2, S3, are transmitted to the transistors only at the rising edge of this clock signal HL, i.e. at the instant when the current for reading or writing the memory cells to be protected will be consumed." 5:26-38 – "Depending on the state of the bits S1, S2, S3, Sa, Sb, the frequency F will assume one of 32 possible values. The sequences of pseudo-random bits, present notably at the outputs S1, S2, S3, will be therefore produced at a frequency that itself varies randomly. This reinforces the random character of the bits produced at the outputs S1, S2, S3, hence the random character of the current consumption of the protection circuit according to the invention. We thus arrive at a very efficient level of protection against the detection of confidential information by the reading of the current consumed at the terminals of an integrated circuit during an operation for reading or writing this information."
(d) an output interface for outputting said cryptographically	3:12-14 – "The present invention seeks to prevent the possibilities of fraudulent use, principally during reading but also optionally of

processed quantity to a recipient thereof;	fraudulent use relating to the writing of confidential information."
(e) a hardware-implemented noise production subunit connected to said source of unpredictable information and configured to expend unpredictable amounts of electricity based on the output of said source of unpredictable information; and	Abstract – "To prevent the fraudulent practice of examining the current consumption at the terminals of the integrated circuit during an operation of reading or writing in the memory, a protection circuit is used." 2:29-40 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit." 3:36-38 – "Each simulation cell is designed to consume either a first current or a second current depending on the output logic level of the flip-flop that controls it." 4:12-15 – "The current consumption of the cells is controlled by the outputs S1, S2, S3 of the generator of pseudo-random sequences which gives bits, at these outputs, that are randomly (in fact, pseudo-randomly) 0 or 1 bits." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."
(f) an activation controller, which may be activated by software contained in said device, to activate and deactivate said expending of	3:49-55 – "The transistors T'1, T'2 and T'3 are inhibition transistors, all controlled by the same inhibition signal INH which enables controlling the instant when the protection signal has to effectively function: when the INH signal blocks the transistors T'1, T'2, T'3, the protection circuit no longer works." 4:16-26 – "However, the simulation transistors T1, T2, T3 are controlled through D-type flip-flops, BD1, BD2, BD3, controlled by a

unpredictable amounts of electricity.	common clock HL which is preferably synchronized with the clocks that control the reading and writing sequences of the memory that it is sought to protect. In this way, the pseudo-random bits generated at the outputs S1, S2, S3, are transmitted to the transistors only at the rising edge of this clock signal HL, i.e. at the instant when the current for reading or writing the memory cells to be protected will be consumed." *See also* U.S. Patent No. 5,944,833 to Ugon at, *e.g.*, 5:46-60.

Claim 11 ('661 Patent)	**U.S. 4,932,053 to Fruhauf**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	Abstract – "The disclosure concerns the safety of the confidential information contained in integrated circuits. In a certain number of integrated circuit applications and, more particularly, in the circuits contained in cards known as "chip cards", it is necessary to prohibit access by unauthorized persons to confidential information stored in a memory of the circuit. To prevent the fraudulent practice of examining the current consumption at the terminals of the integrated circuit during an operation of reading or writing in the memory, a protection circuit is used." 1:11-15 – "In a certain number of integrated circuit applications and, more particularly, in the circuits contained in cards known as "chip cards", it is necessary to prohibit access by unauthorized persons to confidential information stored in a memory of the circuit." 1:59-2:3 – "Consequently, it is possible to partially or totally decipher the confidential content of a memory by observing the current consumed during the reading or writing of this memory. A user with fraudulent intent could measure the current consumed between the general supply terminals (necessarily accessible outside the integrated circuit). As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit." 2:4-12 – "Another example of fraud, this time concerning the writing and not the reading of confidential information, would be the following one: in certain protected circuits, there is provision for the user to introduce an enabling code through a keyboard whenever he

	wishes to use the circuit. To prevent fraud involving all the systematic introduction of every possible code, there is provision for storing an error bit in the memory whenever a wrong code is introduced." 2:29-40 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:59-62 – "Consequently, it is possible to partially or totally decipher the confidential content of a memory by observing the current consumed during the reading or writing of this memory." 1:66-2:3 – "As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit." 2:23-26 – "The present invention seeks to prevent these possibilities of fraudulent behaviour, chiefly in the reading but also, as the case may be, in the writing of confidential information."
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of	1:46-52 – "In fact, the operation for reading a 0 bit does not consume the same amount of current as the operation for reading a 1 bit. The same applies to the writing operation. If the memory is read or written in eight-bit words, the difference between the reading (or writing) of eight 0 bits and the reading (or writing) of eight 1 bits is even greater than that of one bit."

said operation;	2:29-45 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit. The consumption read from the external terminals of the circuit will, in effect, be the superimposition of the real consumption of the memory cells and the pseudo-random consumption of the cells of the protection circuit." 3:26-30– "The protection circuit according to the invention, shown in figure is made on the same integrated circuit substrate as the circuit to be protected, and it is supplied by the same Vcc (high level) and Vss (low level) supply terminals."
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	1:23-27 – "In practice, it has therefore been provided that, when the degree of confidentiality is especially high, the confidential information is processed by a microprocessor contained in the same integrated circuit as the memory." 1:66-2:3 – "As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit." 2:4-9 – "Another example of fraud, this time concerning the writing and not the reading of confidential information, would be the following one: in certain protected circuits, there is provision for the user to introduce an enabling code through a keyboard whenever he wishes to use the circuit." 2:29-31 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form. . . ." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential

	information by reading the overall current consumption of the integrated circuit."
(d) a noise production system for introducing noise into said measurement of said power consumption.	Abstract – "To prevent the fraudulent practice of examining the current consumption at the terminals of the integrated circuit during an operation of reading or writing in the memory, a protection circuit is used." 2:29-40 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit." 3:36-38 – "Each simulation cell is designed to consume either a first current or a second current depending on the output logic level of the flip-flop that controls it." 4:12-15 – "The current consumption of the cells is controlled by the outputs S1, S2, S3 of the generator of pseudo-random sequences which gives bits, at these outputs, that are randomly (in fact, pseudo-randomly) 0 or 1 bits." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."

Claim 12 ('661 Patent)	**U.S. 4,932,053 to Fruhauf**
The device of claim 11 wherein said noise production system	2:67-3:2 – "The pseudo-random generator could be made in a standard way by a series of cascade-mounted flip-flops, the outputs of certain flip-flops being looped back to the inputs of other flip-flops

comprises: (a) a source of randomness for generating initial noise having a random characteristic;	through OR-Exclusive gates."
(b) a noise processing module for improving the random characteristic of said initial noise; and	3:3-5 – "The random character may again be reinforced by the random variation of the clock frequency which controls these flip-flops." 4:57-64 – "The oscillator OSC is a controlled frequency oscillator. The frequency is controlled by a five-bit input signal. These five bits represent a pseudo-random sequence given by the generator GPA itself through its outputs S1, S2, S3, Sa Sb. Thus, the frequency of the oscillator varies pseudo-randomly, so that the random character of the bits S1, S2, S3 is reinforced."
(c) a noise production module configured to vary said power consumption based on an output of said noise processing module.	4:12-15 – "The current consumption of the cells is controlled by the outputs S1, S2, S3 of the generator of pseudo-random sequences which gives bits, at these outputs, that are randomly (in fact, pseudo-randomly) 0 or 1 bits."

Claim 13 ('661 Patent)	**U.S. 4,932,053 to Fruhauf**
The device of claim 12 wherein said noise production system is connected to said processor and is selectively operable under the control of said processor.	2:29-40 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit." 3:49-55 – "The transistors T'1, T'2 and T'3 are inhibition transistors, all controlled by the same inhibition signal INH which enables controlling the instant when the protection signal has to effectively function: when the INH signal blocks the transistors T'1, T'2, T'3, the protection circuit no longer works." Claim 1 – "A circuit for the protection of confidential data of a

	memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."

Claim 22 ('661 Patent)	**U.S. 4,932,053 to Fruhauf**
A device according to claims 1, 4, 7, 9, 11, 14, 15, or 20 wherein said device comprises a smartcard.	1:8-9 – "The invention concerns the safety of confidential information contained in integrated circuits." 1:11-15 – "In a certain number of integrated circuit applications and, more particularly, in the circuits contained in cards known as 'chip cards', it is necessary to prohibit access by unauthorized persons to confidential information stored in a memory of the circuit."

Claim 29 ('661 Patent)	**U.S. 4,932,053 to Fruhauf**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	Abstract – "The disclosure concerns the safety of the confidential information contained in integrated circuits. In a certain number of integrated circuit applications and, more particularly, in the circuits contained in cards known as "chip cards", it is necessary to prohibit access by unauthorized persons to confidential information stored in a memory of the circuit. To prevent the fraudulent practice of examining the current consumption at the terminals of the integrated circuit during an operation of reading or writing in the memory, a protection circuit is used." 1:11-15 – "In a certain number of integrated circuit applications and, more particularly, in the circuits contained in cards known as "chip cards", it is necessary to prohibit access by unauthorized persons to confidential information stored in a memory of the circuit." 1:59-2:3 – "Consequently, it is possible to partially or totally decipher the confidential content of a memory by observing the current consumed during the reading or writing of this memory. A user with fraudulent intent could measure the current consumed between the

	general supply terminals (necessarily accessible outside the integrated circuit). As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit." 2:4-12 – "Another example of fraud, this time concerning the writing and not the reading of confidential information, would be the following one: in certain protected circuits, there is provision for the user to introduce an enabling code through a keyboard whenever he wishes to use the circuit. To prevent fraud involving all the systematic introduction of every possible code, there is provision for storing an error bit in the memory whenever a wrong code is introduced." 2:29-40 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:46-52 – "In fact, the operation for reading a 0 bit does not consume the same amount of current as the operation for reading a 1 bit. The same applies to the writing operation. If the memory is read or written in eight-bit words, the difference between the reading (or writing) of eight 0 bits and the reading (or writing) of eight 1 bits is even greater than that of one bit." 2:29-45 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several

	simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit. The consumption read from the external terminals of the circuit will, in effect, be the superimposition of the real consumption of the memory cells and the pseudo-random consumption of the cells of the protection circuit." 3:26-30– "The protection circuit according to the invention, shown in figure is made on the same integrated circuit substrate as the circuit to be protected, and it is supplied by the same Vcc (high level) and Vss (low level) supply terminals." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."
(b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:59-62 – "Consequently, it is possible to partially or totally decipher the confidential content of a memory by observing the current consumed during the reading or writing of this memory." 1:66-2:3 – "As an example of possible fraudulent behavior in the reading of confidential information: it is possible to read a confidential programme stored in a read-only memory in the integrated circuit, or a confidential enabling code stored in an electrically programmable memory of the circuit." 2:6-9 – "Another example of fraud, this time concerning the writing and not the reading of confidential information, would be the following one: in certain protected circuits, there is provision for the user to introduce an enabling code through a keyboard whenever he wishes to use the circuit." 2:23-26 – "The present invention seeks to prevent these possibilities of fraudulent behaviour, chiefly in the reading but also, as the case may be, in the writing of confidential information."

(c) introducing noise into said measurement of said power consumption while processing said quantity; and	2:29-45 – "The invention proposes a circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit. The consumption read from the external terminals of the circuit will, in effect, be the superimposition of the real consumption of the memory cells and the pseudo-random consumption of the cells of the protection circuit." 3:58-65 – "The simulation transistors are preferably given dimensions such that their consumption (current I) is substantially identically to the consumption of a memory cell of the circuit to be protected (not shown) at the time when this cell is read (if it is sought to protect the confidentiality of information during reading) or written (if it is sought to protect the confidentiality of information during writing)." 4:12-15 – "The current consumption of the cells is controlled by the outputs S1, S2, S3 of the generator of pseudo-random sequences which gives bits, at these outputs, that are randomly (in fact, pseudo-randomly) 0 or 1 bits." 4:22-26 – "In this way, the pseudo-random bits generated at the outputs S1, S2, S3, are transmitted to the transistors only at the rising edge of this clock signal HL, i.e. at the instant when the current for reading or writing the memory cells to be protected will be consumed." Claim 1 – "A circuit for the protection of confidential data of a memory in integrated circuit form, said protection circuit comprising, on the same integrated circuit, several simulation cells capable of being controlled individually, these cells having two current consumption states that differ according to the signal that controls them, and a generator of pseudo-random sequences to control these cells, so that each of them is, pseudo-randomly, in one state or in another, thus making it more difficult to determine confidential information by reading the overall current consumption of the integrated circuit."
(d) outputting said cryptographically processed quantity to	3:12-14 – "The present invention seeks to prevent the possibilities of fraudulent use, principally during reading but also optionally of fraudulent use relating to the writing of confidential information."

a recipient thereof.	

Claim 30 ('661 Patent)	U.S. 4,932,053 to Fruhauf
The method of claim 29 wherein said step of introducing noise comprises: (a) generating initial noise having a random characteristic;	2:67-3:2 – "The pseudo-random generator could be made in a standard way by a series of cascade-mounted flip-flops, the outputs of certain flip-flops being looped back to the inputs of other flip-flops through OR-Exclusive gates."
(b) improving the random characteristic of said initial noise; and	3:3-5 – "The random character may again be reinforced by the random variation of the clock frequency which controls these flip-flops." 4:57-64 – "The oscillator OSC is a controlled frequency oscillator. The frequency is controlled by a five-bit input signal. These five bits represent a pseudo-random sequence given by the generator GPA itself through its outputs S1, S2, S3, Sa Sb. Thus, the frequency of the oscillator varies pseudo-randomly, so that the random character of the bits S1, S2, S3 is reinforced."
(c) varying said power consumption based on said improved initial noise.	4:12-15 – "The current consumption of the cells is controlled by the outputs S1, S2, S3 of the generator of pseudo-random sequences which gives bits, at these outputs, that are randomly (in fact, pseudo-randomly) 0 or 1 bits."